Remarks

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1, 3-9, 11, 13, 17, 19, 21, 23, 25, and 28-29 have been amended. Claims 31-38 have been added to recite further disclosed embodiments of the invention. Claims 1-38 are now pending in the application. Applicants note with appreciation the Examiner's careful reading of the claims and have amended the Claims to overcome any confusion that the Examiner may have had regarding their meaning or antecedent bases.

ARGUMENT

Claims 29-30 are objected to because there is no space between the words "data-stream" and "sent." This objection is moot based on the above amendments.

Claims 3-5 and 7-28 are rejected under 35 U.S.C. § 112, second paragraph, as indefinite for failing to point out and distinctly claim the subject matter of the invention. This rejection is respectfully traversed and Claims 3-5 and 7-28 are believed allowable based on the above amendments and following discussion.

Regarding Claim 3, the Examiner asserts that the data stream identifier is not an option, but a requirement, and the limitation of "one of..." is indefinite. This assertion is not quite accurate. The data stream as recited in the claim may contain information that is sufficient to access the appropriate key on its own, or it may need to be combined with a source stream identifier to have sufficient information to access the appropriate key. This distinction is clearly described in the specification as originally filed. The amendments to this claim overcome the Examiner's rejection.

Regarding Claims 4, 11, 13 and 21, the Examiner cites the same listing style as for Claim 3. In each of these cited claims, there is an optional item which has been clearly identified. The optional elements do not indicate alternative embodiments, but indicate that for a specific embodiment an element may, or may not, be necessary depending on other factors as described in the specification.

PAGE 14/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

For instance, Claim 4 recites "*said operations further include receiving a transmission from said second system that includes data indicating said tag; and sending said keys, and if necessary, said portion of said payload, to said second system based on said transmission.*" (Emphasis added). As is clearly described in the specification, the tag data may indicate that a portion of the payload is not necessary to transmit. Claim 11 recites "*said sending system transferring a first data characterized by said at least one key to said receiving system; and if necessary, said replaced payload portion to said receiving system.*" (Emphasis added). Similar to Claim 4, it is clearly described in the specification that a replaced portion of the payload may not be necessary. Claims 13 and 21 are similarly amended to make clear that the replaced payload portion is optionally sent based on the data stream and other factors disclosed in the specification. Thus, as amended, 4, 11, 13 and 21 overcome Examiner's rejection.

With regard to Claim 5, Applicants thank the Examiner for identifying the recited dilemma. The temporal confusion of how the steps can be "performed before they are performed" is overcome by the above amendments.

With regard to Claims 7-8, and generally, the first device, as recited in the claims, may remove a segment of the payload portion of a data block and replace that segment with a tag. This is shown pictorially in Figure 6B. Thus, when the first device sends the payload to the second device, there may be piece of the original data missing, i.e., the removed segment. The second device receives this removed segment later, after negotiating with the first device to receive session or decryption keys and the removed payload segment. Thus, the second device may receive the same payload portion twice, when necessary. If a tag has been inserted and a segment removed, the missing data is sent the second time. The Claims have been amended to make clear to which portion of the data block they are referring to overcome this rejection.

Claim 9 is rejected because the Examiner asserts that the order of the steps is not the same, leaving the claim indefinite. This rejection is respectfully traversed and amended Claim 9 is believed allowable based on the foregoing and following discussion. Claim 9 recites, in part:

> ***replacing** a portion of a data block payload with at least one tag bits;*
> ***setting** a flag in a header of said data block;*
> ***encrypting** said payload with at least one key; and*

PAGE 15/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

transmitting said data block to a receiving system after said setting a flag, said encrypting, and said replacing.

The Examiner objects because the steps of replacing, setting and encrypting do not appear in the same order as they do in the limitation of transmitting. This assertion is in error because there is no temporal requirement in a method claim unless it is explicitly recited or implied based on inputs and outputs used by, or required by other steps. In this case, the only requirement of the transmitting step is that it occurs after all of the other three recited steps. It is not necessary to the claim that the three steps of setting, encrypting and replacing are performed in a specific order in relation to the transmitting, but just that they occur first. For instance, the setting can easily take place before or after the replacing or encrypting with no loss of functionality, as long as they occur before the transmitting. Thus, Claim 9, as amended, overcomes the Examiner's rejection.

The rejections to Claim 13 are moot based on the above amendments. As recited in the claims and described in the specification, the payload has a portion removed to replace it with tag bits. The original portion is designated as the "replaced payload portion" because it has been replaced with tag bits. The replacement portion is designated as the "payload portion", the antecedent appearing in parent Claim 9 as, "*replacing a portion of a data block payload*" which includes the tag bits. (Emphasis added). The confusion regarding which payload portion is being recited is overcome by the above amendments.

Regarding Claim 16, the recitation of "said keys" is purposely recited. The tag bits may identify the source of all of the keys, i.e., identifying a data stream and optionally a source stream. This identifies the necessary keys required to be sent by the sending system to the receiving system. As is clearly defined in the specification and recited in the claims, more than one type of key may be required to decode the data block. The decryption key may itself be encrypted, requiring a session key. The keys are typically sent to the receiving system via a secondary transmission channel used for non-data block information, and the source of any and all of the required keys is defined by the tag bits.

The rejections to Claims 17, 19 and 23 are moot based on the above amendments and discussion.

PAGE 16/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

Claims 1-30 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,908 to Cooper et al., (hereafter, "Cooper et al."). This rejection is respectfully traversed and Claims 1-30 are believed allowable based on the above amendments and the foregoing and following discussion.

Generally, Cooper et al. teach a system for enabling a file or software application which has been locked from the user. Cooper et al. teach an apparatus for securing access to particular files which are stored in a computer-accessible memory media. A plurality of files is stored in a computer-accessible memory media, including at least one encrypted file and at least one unencrypted file. For each encrypted file, a *preselected portion of the file* is recorded in memory, a decryption block is generated which includes information which can be utilized to decrypt the file, and the decryption block is incorporated in the file in lieu of the *preselected portion* which has been recorded in memory.

In contrast, Applicants' invention recites a system for transmitting a data stream made up of data blocks, where a data block portion of a payload may be replaced with a tag indicating whether a decryption key is necessary to decode the data block. The data blocks of a given data stream may contain disparate protocols and be routed to one or more application decoders. Further, the sending device and receiving device may negotiate for a session key to decrypt the decryption keys, thereby enabling additional security to the data stream as is passes through the data safeguarding device.

Cooper et al. teach a system where only one portion of a file is encrypted to protect it from being accessed by a user upon a user request to access the file. An operating system level file management program determines whether the user is authorized to access the file and supplies the decryption key. Cooper et al. teach supplying the key by the vendor. Cooper et al. do not teach or suggest that the decryption key is further encrypted by a negotiated session key, nor do they teach a data stream received from a source device, but merely a file drawn from media.

As described in the specification, and recited in the claims, Applicants' invention safeguards data within a device and forwards data of varying protocols to appropriate application decoders. If a data stream contains both audio and video data blocks, the data blocks from the received data stream may be sent to different application decoders based on their protocol, i.e.,

PAGE 17/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

audio vs. video formats. Applying the teachings of Cooper et al. to Applicants' invention will result in an operating system level decoder for files and not a safeguarding device that may be implemented in hardware, software, or firmware that receives transmitted data streams without user request.

With regard to Claims 1, 9, 14, 19 and 21, the Examiner asserts that Cooper et al. disclose all elements of the claims. Applicants' claims require that the first system comprises a protected content exchange (PCX) module, and the second system comprises at least one application decoder module. Cooper et al. does not teach that the first system is a PCX, nor that the second system is one or more application decoder modules. The Examiner asserts that Cooper et al. teach encrypting the payload (Col. 3, lines 55-57). Cooper et al. do not teach *said sending system encrypting said payload with at least one key*, as recited in the claims. Cooper et al. teach a system where an external source encrypts the file and supplies a pre-encrypted file and pre-selected portion to be stored on the file system of a user's computer. Cooper et al. do not teach a method to re-encrypt a decrypted data stream, but only a method to decrypt a file on a media device. In contrast, Applicants' claimed invention receives a data stream and encrypts the payload portion of the data blocks in the data stream before sending them to one or more application decoders. The PCX and application decoders may be separate devices, circuits or modules, or they may be part of the same device. Regardless, the PCX and application decoders are part of an overall data safeguarding system. Cooper et al. teach that the encryption occurs on a vendor system and decryption occurs on a user system.

Similarly, regarding Claims 2, 10 and 20, Cooper et al. do not teach the act of encrypting a portion of the payload in Col. 3, lines 57-59. Cooper et al. teach that a pre-encrypted file is placed in memory and a decryption block is generated to facilitate decryption. Thus, applying Cooper et al. to Applicants' invention would not yield a data safeguarding system which maintains encrypted data to be transmitted within the device. Applying the teachings of Cooper et al. would allow Applicant to decrypt a file and data safeguarding would end once the file had been decrypted.

Regarding Claims 3 and 16, the Examiner equates a tag including a data stream and key identifier with Cooper's name for a key file. A name for a file containing keys is not the same as a tag identifying a data stream identifier and a key identifier. The tag as recited by Applicants'

PAGE 18/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

claims requires a data stream comprising data blocks. The files taught by Cooper et al. do not contain data blocks as described by Applicants where each data block has a header and payload portion. The encrypted file of Cooper et al. is an entire file encrypted by a key. Data blocks of the files are not separately transmitted, or encrypted with separate keys, as enabled by Applicants' claimed invention.

Regarding Claims 4, 6-8, 11-13, 17, 18, 22-25, 27, 29 and 30, the Examiner misinterprets which system is performing which tasks. The Examiner fails to note that Applicants' invention comprises two (2) "systems" which negotiate non-data block information including keys, and encrypted data blocks or tag information are passed to one another. For instance, in Claim 4, Applicant recites *receiving a transmission from said second system that includes data indicating said tag; and sending said keys, and if necessary, said portion of said payload, to said second system based on said transmission*. Applicants' invention negotiates between the two systems to determine a decryption key required by the second system (application decoder) for each data block, where after receiving the tag, the first system (PCX device) sends the second system the appropriate decryption key(s), session key (if necessary) and a portion of the payload, if it has been replaced by a tag and needs to be restored. Cooper et al. (Col. 4, lines 12-22) teach a system that decrypts a file by decoding a decryption block by a file management system using a key file. The file management system then sends on the unencrypted file, in whole, and the user may then use the unencrypted file. The file is not safeguarded as it passes through the system unencrypted, nor are two systems disclosed in the reference as cited by the Examiner.

Regarding Claims 5 and 28, the Examiner asserts that Cooper et al. teach receiving a stream of data from a third system. (Col. 3, lines 9-15) Cooper et al. do not teach receiving a data stream, whether from a third system or elsewhere. Cooper et al. (Col. 3, lines 9-15) teach receiving a *software object* from a source. Cooper's software object is not analogous to a data stream comprising data blocks which may be sent and decrypted separately. Further, even if Cooper's software object could be transmitted in blocks, it must be reassembled into one piece and decoded as one object in order for it to function as a software executable, or object. Further, Applicants' invention recites a second system comprising at least one application decoder module. Applicant further discloses that separate data blocks within the same data stream may

PAGE 19/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

be sent to one or more (at least one) application decoders, thus, not maintaining the data stream as one entity, as taught by Cooper et al.

Regarding Claims 15 and 26, the Examiner asserts that Cooper et al. teach that the system can be a network of computers. This is in fact not what Cooper et al. teach in Column 21, lines 20-26. Cooper et al. teach that a user's computing device, which as a whole, acts as the decryption device, may be on a computer network. The network is not relevant to the functioning of Cooper's device. Cooper et al. teach that a decryption key may be stored on another system on the network, or supplied by a system administrator. Manually supplying a key from an administrator does not result in Applicants' claimed invention. Further, the systems on a computer network as taught by Cooper et al. do not negotiate for session and decryption keys using tag information. Moreover, the systems on a computer network do not re-encrypt payload data of data blocks for transmission from a PCX device to one or more application decoders. Applicant discloses and claims that *said sending system and said receiving system are separate physical devices*. As described in the Specification, the devices of the sending system and receiving system are not computer networks, but devices within the same data safeguarding system – not *network*.

Thus, for the foregoing reasons, all claims remaining in the application are now allowable.

PAGE 20/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14

CONCLUSION

In view of the foregoing, Claims 1-38 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 2 Jul 2004

Joni D. Stutman-Horn
Patent Attorney
Intel Corporation
Registration No. 42,173
(703) 633-6845

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

PAGE 21/21 * RCVD AT 7/2/2004 6:52:32 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:4087208381 * DURATION (mm-ss):09-14